PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-341151
(43)Date of publication of application : 10.12.1999

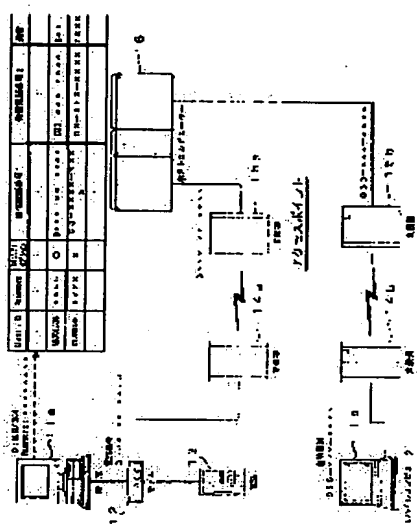
(51)Int.CI. H04M 1/66
G06F 15/00
H04M 11/00

(21)Application number : 10-150114
(22)Date of filing : 29.05.1998

(71)Applicant : NEC CORP
(72)Inventor : ISHIKAWA YOSHIHARU

(54) DIAL-UP CONNECTION AUTHENTICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To more surely confirm account in an Internet connection and a personal communication service by the way of dial-up.
SOLUTION: A user side terminal 11a operates dialing to an access point at a service provider side. A called telephone number is communicated to a host computer 16. Also, when a line is connected, a user ID and a password are transmitted to the host computer 16. In the host computer 16, the user ID and the password are confirmed in the same way at the time of normal connection, and the called telephone number is checked without starting the service provision, and when they are matched with each other, the connection is authenticated, and each kind of service provision is started.



LEGAL STATUS

[Date of request for examination]	29.05.1998
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3161414
[Date of registration]	23.02.2001
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－341151

(43)公開日　平成11年(1999)12月10日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｍ　1/66		Ｈ０４Ｍ　1/66	Ｃ
Ｇ０６Ｆ　15/00	３１０	Ｇ０６Ｆ　15/00	３１０Ｃ
Ｈ０４Ｍ　11/00	３０３	Ｈ０４Ｍ　11/00	３０３

審査請求　有　　請求項の数３　ＯＬ　（全６頁）

(21)出願番号　特願平10－150114

(22)出願日　平成10年(1998)５月29日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　石川　義晴
東京都港区芝五丁目７番１号　日本電気株式会社内

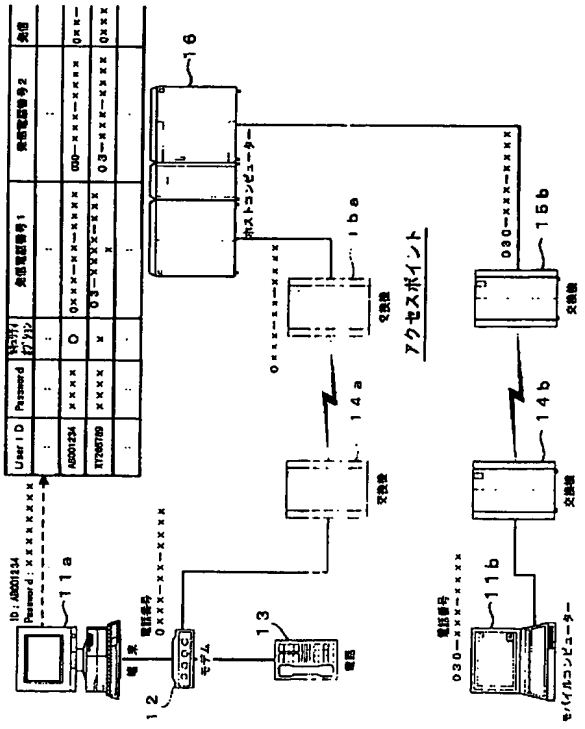
(74)代理人　弁理士　高橋　詔男　（外３名）

(54)【発明の名称】　ダイヤルアップ接続認証方式

(57)【要約】

【課題】　ダイヤルアップによるインターネット接続やパソコン通信サービスにおいて、より確実なアカウントの確認を行う。

【解決手段】　ユーザ側端末１１ａは、サービス提供者側のアクセスポイントに対してダイヤリングを行う。このとき、発信電話番号がホストコンピュータ１６へ通知される。また、回線が接続されると、ユーザＩＤとパスワードがホストコンピュータ１６へ送信される。ホストコンピュータ１６では、通常の接続時と同様にユーザＩＤ、パスワードの確認を行った後、そのままサービス提供を開始せずに、さらに、発信電話番号をチェックし、一致すれば、接続を認証して各種サービス提供を開始する。



【特許請求の範囲】
【請求項１】　ダイヤルアップにより接続要求してきた端末に対してユーザ認証を行うダイヤルアップ接続認証方式において、
予め、ユーザ毎の発信電話番号を記憶しておき、前記端末から接続要求があると、着信時に通知される前記端末の発信電話番号と予め記憶していた発信電話番号とを比較し、双方が一致するか否かを判断することでユーザ認証を行うことを特徴とするダイヤルアップ接続認証方式。
【請求項２】　前記ユーザ認証の前後に、回線接続後に端末から送信されるユーザＩＤおよびパスワードと予め登録されているユーザＩＤおよびパスワードとを比較し、それぞれ双方が一致するか否かを判断することで第２のユーザ認証を行うことを特徴とする請求項１記載のダイヤルアップ接続認証方式。
【請求項３】　着信時に通知される前記端末の発信電話番号と予め記憶していた発信電話番号とを比較し、双方が一致した場合、少なくとも予め記憶していた発信電話番号を含むユーザ情報の更新を許可することを特徴とする請求項１記載のダイヤルアップ接続認証方式。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ダイヤルアップによるインターネット接続やパソコン通信サービスにおいて、サービス提供者／プロバイダが回線接続時にサービス利用者のアカウントを確認するためのダイヤルアップ接続認証方式に関する。
【０００２】
【従来の技術】ダイヤルアップによるインターネット接続やパソコン通信サービスにおいては、ユーザ端末側からサービス提供者側のアクセスポイントに対し、ダイヤリングを行い、サービス提供者側は、ユーザ端末側から送信されるユーザＩＤ及びパスワードにより、そのユーザ認証を行ってサービス提供を開始する。
【０００３】
【発明が解決しようとする課題】しかしながら、従来技術では、第三者にユーザＩＤとパスワードが漏洩し、不正に利用された場合、サービス提供者はサービス利用時間や特定のサービス利用の内容に応じて、ユーザＩＤを持つ利用者に対して利用料として課金を行うため、ユーザＩＤの不正利用により、正規ユーザが多大な損害を受けてしまうという問題があった。
【０００４】この発明は上述した事情に鑑みてなされたもので、ダイヤルアップによるインターネット接続やパソコン通信サービスにおいて、サービス提供者／プロバイダが回線接続時にサービス利用者のアカウントを確認する際に発信電話番号通知情報を利用して、より確実なアカウントの確認を行うことができるダイヤルアップ接続認証方式を提供することを目的とする。
【０００５】
【課題を解決するための手段】上述した問題点を解決するために、請求項１記載の発明では、ダイヤルアップにより接続要求してきた端末に対してユーザ認証を行うダイヤルアップ接続認証方式において、予め、ユーザ毎の発信電話番号を記憶しておき、前記端末から接続要求があると、着信時に通知される前記端末の発信電話番号と予め記憶していた発信電話番号とを比較し、双方が一致するか否かを判断することでユーザ認証を行うことを特徴とする。
【０００６】また、請求項２記載の発明では、請求項１記載のダイヤルアップ接続認証方式において、前記ユーザ認証の前後に、回線接続後に端末から送信されるユーザＩＤおよびパスワードと予め登録されているユーザＩＤおよびパスワードとを比較し、それぞれ双方が一致するか否かを判断することで第２のユーザ認証を行うことを特徴とする。
【０００７】また、請求項３記載の発明では、請求項１記載のダイヤルアップ接続認証方式において、着信時に通知される前記端末の発信電話番号と予め記憶していた発信電話番号とを比較し、双方が一致した場合、少なくとも、予め記憶していた発信電話番号を含むユーザ情報の更新を許可することを特徴とする。
【０００８】この発明では、サービス利用者からの着信の度に発信電話番号と登録済みの発信電話番号とを照合する。したがって、第三者によるアカウントの不正利用を防止することが可能となる。
【０００９】
【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。
Ａ．実施形態の構成
図１は、本発明の実施形態による全体の構成を示すブロック図である。図において、端末１１ａは、ユーザ側の固定端末であり、モデム１２により発信し、交換機１４ａを介して電話網に随時接続する。モデム１２には、通常の電話機も接続することが可能である。この場合、端末１１ａからのホストコンピュータ１６への発信は、常時、同じ発信電話番号となる。交換機１４ａは、図示の例では発信側の交換機であり、電話網に接続され、モデム１２による発信に従って、着信側の交換機１５ａに接続する。また、交換機１５ａは、図示の例では着信側（サービス提供者側）の交換機であり、電話網に接続され、交換機１４ａからの着信を受け付け、ホストコンピュータ１６に接続する。
【００１０】また、端末（モバイルコンピュータ）１１ｂは、ユーザ側の移動端末であり、その位置に応じた交換機１４ｂを介して電話網に随時接続する。この場合、端末１１ｂからのホストコンピュータ１６への発信は、その都度、異なる発信電話番号となる可能性がある。交換機１４ｂは、図示の例では発信側の交換機であり、電

話網に接続され、モバイルコンピュータ１１ｂからの発信に従って、着信側の交換機１５ｂに接続する。また、交換機１５ｂは、図示の例では着信側（サービス提供者側）の交換機であり、電話網に接続され、交換機１４ｂからの着信を受け付け、ホストコンピュータ１６に接続する。

【００１１】サービス提供者側のホストコンピュータ１６は、ユーザ認証を行うために、ユーザＩＤ、パスワード、セキュリティオプションフラグ、複数の発信電話番号、を対応付けてユーザプロファイル情報として記憶している。ホストコンピュータ１６は、着信側交換機１５ａ，１５ｂから通知される発信電話番号と登録済みの発信電話番号との比較を行う。発信電話番号は、１９９８年２月より全国的に開始されている、着信者側に発信者側の電話番号を通知するサービスにより、交換機１４ａ、１５ａ（または１４ｂ、１５ｂ）を介して着信者側に通知される。なお、ホストコンピュータ１６に記憶されているユーザ認証用のユーザプロファイル情報の詳細については後述する。

【００１２】次に、図２は、図１に示すサービス提供者側のアクセスポイント及びホストコンピュータの詳細な構成が示すブロック図である。図２において、中継装置２２は、電話網２１から着信を受け付け、それとともに発信電話番号の通知を受ける。通知された発信電話番号を発信電話番号記憶部２３へ退避するとともに専用線等の回線を通じ、ホストコンピュータ１６との通信を開始する。また、ユーザ端末側１１ａとサービス提供者側のホストコンピュータ１６とのユーザＩＤ、パスワードの認証確認後、発信電話番号記憶部２３に退避した発信電話番号をホストコンピュータ１６へ送信する。

【００１３】サービスマネージャ２４は、ユーザ端末１１ａ側から送信されるユーザＩＤを受信し、ホストコンピュータ１６上に記録されているユーザプロファイル情報２６を参照する。続けて、ユーザ端末側からはユーザ固有のパスワードが送信されるので、受信したパスワードとユーザプロファイル情報２６に記録されている情報が一致することを確認する。ここでの情報の不一致が生じた場合には、ユーザ端末１１ａ側に対し、パスワードの再入力を要求する等の復旧手段を講ずる必要があるが、本発明の適用範囲外であるためその詳細についての説明は省略する。

【００１４】パスワードによる認証確認後、アクセスポイントの中継装置２２から発信電話番号記憶部２３に退避されている発信電話番号を受信し、発信電話番号管理部２５へ退避するとともにユーザプロファイル情報２６に定義されている１つ以上の登録発信電話番号および発信電話番号の確認（発信電話番号確認機能）を行うか否かを明示するフラグ（セキュリティオプションフラグ）を参照し、その設定内容に応じて、追加のユーザ認証を行う。ここでセキュリティオプションフラグ及び１つ目の登録発信電話番号（第一登録発信電話番号）のデフォルト値は、各々、発信電話番号の確認を行わない設定、サービス利用申請時の登録電話番号となっている。

【００１５】利用者が発信電話番号確認機能を利用するためには、ユーザプロファイル情報２６に定義される第一登録発信電話番号の回線からユーザ端末１１ａ側が通信サービスを利用し、これらの情報を変更する。ユーザ端末１１ａ側から、これらのセキュリティ情報の変更が要求されると、発信電話番号管理部２５に退避してある発信電話番号とユーザプロファイル情報２６に含まれる第一登録発信電話番号とを比較し、一致した場合に限り、ユーザプロファイル情報２６に含まれる、これらのセキュリティ情報の更新を可能とする。利用者は、複数の登録発信電話番号を登録しておくことにより、携帯電話等を使用したモバイルコンピュータ１１ｂにより、外出先から通信サービスを利用することが可能となる。

【００１６】Ｂ．実施例の動作

次に、図３に示すフローチャートを参照して本実施例の全体の動作について詳細に説明する。まず、図１のユーザ側端末１１ａから、サービス提供者側のアクセスポイントに対してダイヤリングを行う。サービス提供者側は、アクセスポイントの中継装置２２において、電話網２１から着信を受けるとともに発信電話番号の通知を受けることが可能である。中継装置２２は、専用線等の回線を通じて、ホストコンピュータ１６と通信を開始するとともに、発信電話番号記憶部２３に着信時に通知された発信電話番号を記憶する（ステップＳ３１）。

【００１７】ホストコンピュータ１６側で一連のサービス提供を制御するサービスマネージャ２４では、通常の接続時と同様にユーザＩＤの確認を行い（ステップＳ３２）、ユーザプロファイルデータ情報２６を参照し、パスワード確認を行う（ステップＳ３３）。パスワード確認後、そのままサービス提供を開始せずに、さらに発信電話番号の確認を行う（ステップＳ３４）。該発信電話番号確認処理について以下に詳細に説明する。

【００１８】次に、図４は、図３の発信電話番号確認処理（ステップＳ３４）の詳細な動作を説明するためのフローチャートである。まず、アクセスポイントの中継装置２２からステップＳ３１で発信電話番号記憶部２３に退避していた発信電話番号を受信し、発信電話番号管理部２５へ退避するとともに、ステップＳ３２で取得済みのユーザＩＤに対応するユーザプロファイルデータ情報２６から発信電話番号確認を行うための情報（発信電話番号情報）を取得する（ステップＳ４１）。

【００１９】次に、ステップＳ４１で取得した発信電話番号情報の１つである発信電話番号確認サービスの利用の有無を判別するためのフラグを参照し、本サービスを利用しない設定に定義してある場合には、そのまま接続を認証し、各種サービス提供を開始する（ステップＳ４２）。一方、本サービスを利用する設定にしてある場合

には、ユーザプロファイル情報２６に設定されている発信電話番号情報をチェックし（ステップＳ４３，ステップＳ４４）、一致するものがあれば、接続を認証し、各種サービスプログラム２７によるサービス提供を開始する。これに対して、一致するものがなければ、第三者による不正利用と見なし、回線切断処理を行う（ステップＳ４５）。

【００２０】次に、図５は、サービス提供者側のホストコンピュータ１６上にあるユーザプロファイル情報２６に定義されている発信電話番号情報を更新する際の処理の動作を説明するためのフローチャートである。ユーザプロファイル情報２６に定義されている発信電話番号情報を更新する際には、まず、発信電話番号管理部２５に退避された発信電話番号とユーザプロファイル情報２６に含まれる第一登録電話番号とを比較し（ステップＳ５１）、これらの情報が一致している場合に限り、セキュリティオプションフラグ及び登録電話番号情報の更新を認める（ステップＳ５２）。また、発信電話番号が不一致の場合には、ユーザ端末１１ａに対して、発信電話番号情報の更新ができない旨、通知を行う（ステップＳ５３）。

【００２１】Ｃ．他の実施例

次に、本発明の他の実施例について説明する。上述した実施例においては、発信電話番号が登録済みのデータと一致することを確認し、ユーザ認証を行う方法と登録情報の更新手段とについて説明したが、引越などにより、利用者の電話番号の変更が余儀なくされる場合があり得る。このような場合には、容易に利用環境の移行ができる必要がある。

【００２２】そこで、通常利用する登録発信電話番号とは別に移行予定の発信電話番号（予約発信電話番号）を登録しておき、発信電話番号確認手順のステップＳ４３において、この予約発信電話番号も比較対象とし、さらに予約発信電話番号と着信時の発信電話番号が一致した場合に限り、第一登録発信電話番号の情報を予約発信電話番号で置き換える。この手順を踏むことにより、以降、何の影響もなくサービスを受けることが可能となる。

【００２３】また、上述した実施例においては、発信電話番号確認処理をパスワードの確認後に行うものとして説明した。しかしながら、発信電話番号の確認時に接続拒否となるケースでは、パスワードの入力／確認処理は無意味なものとなってしまう。このため、発信電話番号の確認処理は、パスワードの確認前に行う形態としてもよい。

【００２４】

【発明の効果】以上説明したように、本発明によれば、サービス利用者からの着信の度に発信電話番号通知情報と登録済みの発信電話番号とを照合するようにしたので、より確実なアカウントの確認を行うことができ、第三者によるアカウントの不正利用を防止することができるという利点が得られる。

【図面の簡単な説明】

【図１】　本発明の実施形態による全体の構成を示すブロック図である。

【図２】　サービス提供者側のアクセスポイント及びホストコンピュータの詳細な構成が示すブロック図である。

【図３】　サービス提供者側ホストコンピュータにおける通信サービス開始前の接続確認処理の基本的な動作を示すフローチャートである。

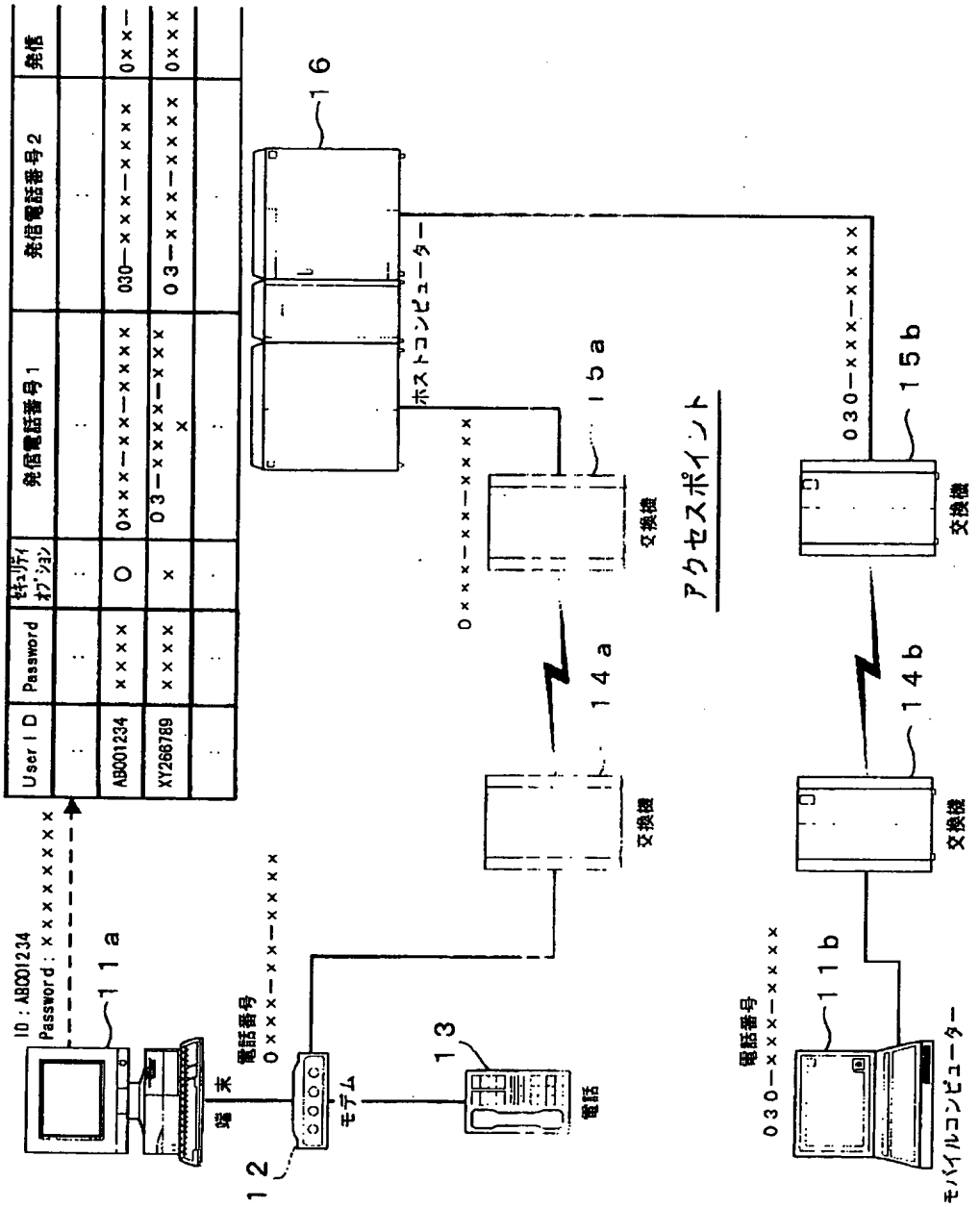
【図４】　発信電話番号確認処理（ステップＳ３４）の詳細な動作を説明するためのフローチャートである。

【図５】　ユーザプロファイル情報２６に定義されている発信電話番号情報を更新する際の処理の動作を説明するためのフローチャートである。

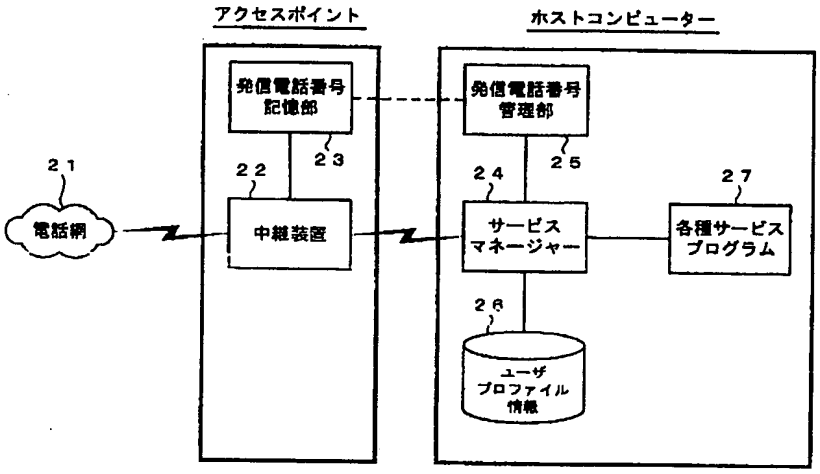
【符号の説明】

１１ａ，１１ｂ　端末
１２　モデム
１３　電話
１４ａ、１５ａ、１４ｂ、１５ｂ　交換機
１６　ホストコンピュータ
２１　電話網
２２　中継装置
２３　発信電話番号記憶部
２４　サービスマネージャ
２５　発信電話番号管理部
２６　ユーザプロファイル情報
２７　各種サービスプログラム

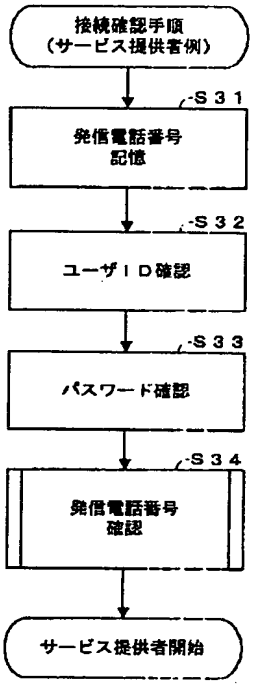
【図１】


User ID
Password
特ユリティオプション
発信電話番号1
発信電話番号2
発信
ABC01234
XY2668789
ホストコンピューター
アクセスポイント
交換機
電話
モデム
端末
モバイルコンピューター
ID：ABC01234
Password：××××××××
電話番号
0××−××−××××
030−×××−××××
11a
11b
12
13
14a
14b
15a
15b
16

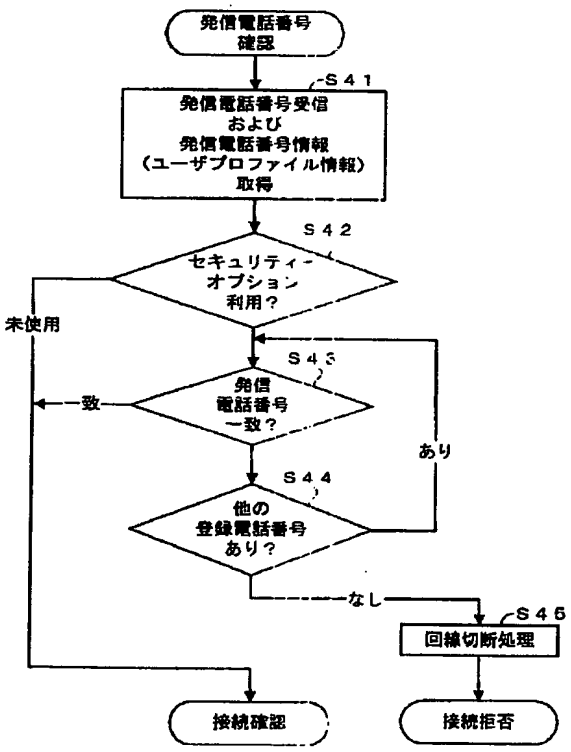
【図２】



【図３】



【図４】



【図５】